A Novel Approach for Detecting DDoS using Artificial Neural Networks.

Abdullah Aljumah, Tariq Ahamad
College of Computer Engineering & Sciences Prince Sattam Bin Abdulaziz University, KSA

Abstract
DDoS attacks are the perfect planned attacks with the aim to stop the legitimate users from accessing the system or the service by consuming the bandwidth or by making the system or service unavailable. The attackers do not attack to steal or access any information but they decline the performance of the network and the system. DDoS attack at application layers are difficult to detect because they imitate the legitimate traffic. We used Lyapunav coefficient to check the traffic and patter for being attack traffic or legitimate traffic and a six step technique is designed using chaos theory to secure networks from DDoS attack traffic. In this research article we have proposed a novel approach of detecting DDoS attack using artificial neural network and theory of chaos.

Keywords:
ANN, DDoS, IDS,

1. Introduction

With the advent of latest networking technology especially the internet, whole world is becoming more inter-connected than ever before. The worldwide networking infrastructure hosts extremely large amount of governmental, personal, military and commercial information. Network security is a major concern which is an inherent property acquired by the internet [1].

In the previous years, enormous security augmented methods have been devised to enhance the security of the transmission of data over the publicly networks. Currently, cryptographic algorithms, system augmented methods of routing and system infrastructure tremendously enhance data transmission..The common objectives of these techniques usually are to defeat diverse threats facing the internet which are spoofing, eavesdropping, session hijacking and many more.

Wireless networks are the demand of the situation for any type of arising businesses. Similarly, it's necessary for a well-established business firm to enhance their IT infra by integrating the wireless networks to achieve technological superiority over their competitors. The above argument is supported by the fact that wireless data networks enhance the business with their properties of flexibility, mobility and extensibility. Alongside, it saves the costs considerably in the comparison of conventional wired networks. Nevertheless, organizations must be fully proficient to confront the problem which arises with wireless data networks. Denial of Service (DoS) attacks is obvious in wireless data networks. In the modern day systems safeguarding against DoS attacks need to be considered as a crucial part of any security system. The DoS attacks are more dangerous than the threats like worm, virus, malware etc which subverts the advantages that are associated with wireless networks. The reason for this network degradation is due to the fact that transmission medium in wireless networks is shared which is susceptible to DoS attacks. Although, conventional DoS attacks involve flooding a host with more service requests, whereas, in case of wireless networks the routing strategies between the participating nodes and limited bandwidth creates unusual ways for projecting DoS attacks. The impact of DoS attacks is so severe that it could bring down the network partially or entirely.

2. Security and Attack Types

Security: Security in wireless mobile networks is hard to obtain due to link vulnerabilities, insufficient physical defense, dynamic topological changes and the irregularity in the connectivity. The frequent topological changes among the communicating nodes also changes the trust relationship between them, consequently, the security mechanism with the static type configuration won't be sufficient [2].

Security does not concern only to the participating nodes in the network. During the data transmission the communication links should not be susceptible to any type of attack. A potential hacker can target a communication channel, retrieves the secret keys, decrypt them and injects false data in the network. The network security is important just like the security of computers and the encryption of the messages. In order to develop secure network few points need to consider which are as under [3]:

- Confidentiality: The data is the network persists to be private.
- Access: Only the authorized users have access to communicate over the network.

Manuscript received December 5, 2016
Manuscript revised December 20, 2016

- Integrity: Ensures the data in transit is not modified and reaches destination in actual form.
- Authentication: Ensures the users in the network are those, who they claim to be.
- Non-repudiation: Ensures the user doesn't contradict that he has used the network.

***Attacks*:** Generally internet attacks are classified into many categories. Phishing and eavesdropping attacks are carried out to gain the personal information and system knowledge. Some attacks like worms, viruses and Trojans are perpetrated to alter the systems aimed function. DoS is a type of attack in which the system resources are consumed so heavily that makes the system inoperative.

Table 1: Attack types and Security methods [4]

Security characteristics	Attacks Types	Security methods
Privacy	DoS,Email Bombing, Spamming, Hacking, and cookies	IDS, firewall, Anti-malwares, software, IPSec, SSL
Integrity	Viruses, Worms, Trojans, Eavesdropping, DoS, IP spoofing	IDS, firewall, Anti-malwares, software, IPSec, SSL
Availability	DoS, Email bombing, Spamming, System boot record infectors	IDS, Anti Malware, software, firewall
Confidentiality	Eavesdropping, Hacking, Phishing, DoS, IP spoofing	IDS, Firewall, Cryptographic systems, IPSec, SSL

***Eavesdropping*:** When an unauthorized person intercepts the communication is known as eavesdropping. Eavesdropping can be passive or active, in the former case the intruder only listens to the channel passively, and in the latter case the intruder first listens and then injects some stealth data in the communication. This result could be the distorted information or secret information can be snipped away. [4].

***Worms*:** Worms and viruses have a similar property of self-replicating. But, the former doesn't require a file to replicate itself and propagate throughout the system [4].Network ware worms and mass-mailing are two main types of worms. A network aware worm chooses a target and typically infects it by a Trojan or other. In mass mailing worms email is a means to infect the target.

***Viruses*:** Viruses can infect the files and propagates throughout the system[4] by replicating themselves.

***Trojans*:** Trojans seem to be harmless for the system, but carries some malicious intention**.** They normally transport some payload like virus [4].

***Phishing*:** Phishing is an effort to retrieve the information which is confidential from a person, a group, or an organization [5]. The person who carries out phishing attacks deceits the user to reveal his personal information, banking data, credit card numbers and other secret information.

IP Spoofing Attacks: In this type of attack the address of an authorized computer is copied to look legitimate node in order to gain the access to other computers in the network. The id of the adversary remains hidden by distinctive ways which makes the prevention and detection difficult. With the current network security provisions, IP spoofed attacks cannot be avoided [4].

Denial of Service: Denial of Service is an attack that aims to interrupt the normal functioning of the network. In this type of attack huge number of malicious data packets is injected in the network. The network nodes receive them and put forth to the neighboring nodes. It's actually a multilayer type of attack [6]. In Wireless sensor networks there are different types of DoS attacks in distinct layers like collision, tampering, and jamming etc.

3. Literature Review

In [7], the game theory scheme which is based upon UDSR (Utility based dynamic source routing) is employed as secured routing protocol that is adopted from DSR (Dynamic Source Routing) and also Watch list is employed for the identification of a malicious node. To select the secure route, utility value is used and to measure the node misbehavior, reputation and cooperation is also employed. By comparing the loss of packets in UDSR and regular DSR the former loses less. The reason behind the loosing of more packets in DSR is that, it doesn't react to the malicious behavior of the packets, whereas, UDSR and watch list isolates the bad node and label it as malicious. This malicious node doesn't harm the underlying network anymore. The major concerns with this framework are how to set the threshold values and avoid the incorrect labeling.

In [8], majority of the techniques of attack prevention are based upon game theory, soft computing, multi-agent, and artificial intelligence approaches. Decision tree and fuzzy Q-learning approaches are used in soft computing techniques. In game-theory approach a technique is proposed for every possible scenario and Nash equilibrium is the answer. Dendritic cells and danger theory is used in artificial intelligence. Multi-agent immune system has every agent with defined goals and duties.

In [9], Auction theory is employed for the detection of non-cooperative nodes. UDSR approach is used in this protocol. Bid price is used instead of utility value to select secure route. The resultant protocol is termed as SAR (Secure Auction based Routing). To identify a malicious node in the network, destination uses timeout timer. Before a packet reaches to the destination, if the timer is expired, a message with bad route to the base node and all other nodes in the network will be added in the watch list. If a particular nodes appears more than a previously specified number of times, the base station add that node into it's ignore list and broadcasts the list. The dropped average number of packets stays constant in SAR, because the majority of the nodes ignore the bad reputation nodes. Fewer numbers of packets is lost in SAR due to malicious nodes, because of its reaction against the bad behavior. SAR faces same issues like UDSR, threshold values and false labeling.

In [10], The Ad-hoc On demand Distance Routing with Hello flood Detection cum Prevention (AODV-HFDP) differentiated with the existing system. In the system more learning parameters could be added, in order to improve the learning abilities. The authors claim the proposed immune based system will improve the existing Co-FAIS by the addition of two learning parameters in fuzzy system. It improves the detection rate, the accuracy and also improves the learning capabilities. In their proposed system they modified the number of learning parameters. The introduced two new parameters in the existing Co-FAIS i. e. Throughput and Sleep Interval. It improves the accuracy of the system and reduces the false alarm rate.

In [12], HEED (Hybrid Energy-Efficient Distributed clustering) protocol is employed for the cluster forming of sensor nodes. A CH is chosen by employing two cluster parameters, remaining energy of every node in the cluster and communication cost in between a cluster that is a function of cluster density and node degree. This protocol enhances the network life time than LEACH.A node which fails to do mutual authentication is considered to be a malicious node. If a node is detected protocol is devised for the detection of the node which launches hello flood attack. in the network. This is a network layer attack. Indicating the presence of the node a hello message is used. Every node in the network updates its neighbor table on receiving this message which points to the route towards the base station. To differentiate among a friend or a stranger a method which is based on simple test packet is implemented. The receiver of hello message sends back a simple test packet to the sender of hello message; if the reply reaches back in a certain time threshold then it is considered as a friend otherwise a stranger. When the node is declared as malicious, the information about the hello sender node is deleted from the table and also broadcasted in the network. In response to this broadcast, all the nodes in the network delete the information in their routing tables. AODV-HEDP provides more packet delivery ratio as compared to AODV, but it operates for fixed-signal strength, and homogeneous sensors.

In [11], Co-FAIS(Cooperative Fuzzy Artificial Immune System) with some modification is proposed as an immune based system for Denial of Service (DoS) attack on Wireless sensor networks. Co-FAIS is the first intrusion detection model which works in real time. Using the fuzzy logic technique, it detects the attack by comparing the current system with the normal system. Nevertheless, it comprises few disadvantages which are; it doesn't have learning capabilities and is built on one normal model that doesn't improve the detection over the time. So, the normal model needs to be updated which is

by a CH as compromised or malicious; it requests the KDS (Key distribution server) to interrupt the operations of that node. In response, KDS removes the secret key from its list of records, which renders the nodes as keyless. In the result, all the provided services are cancelled and also blocked for any type of future requests. CHs transmit an encrypted message to other CHs to block the detected node for further inter-cluster communication. The other clusters in the network function normally. This proposed protocol does not defend only the wsn network against the DoS attack but also keeps integrity, confidentiality, authenticity between nodes. If an attacker is aware about the detection mechanism then any cluster can be made malicious. The authors claim that the technique is efficient as well as accurate.

In [13], Bayesian game is used to secure LEACH protocol which is known as S-LEACH. It has many rounds, which starts with the phase setup then continues to steady phase. Cluster heads are chosen in the setup phase. In the next phase, these CHs use Time Division

Multiple Access (TDMA) approach for the assignment of time to the sensor nodes of their cluster to send the data. The central intrusion detection system is informed by local IDS about the presence of malicious nodes. In turn, the central IDS notifies whole network about the presence of malicious node. In order to prevent system resources from any wastage, local IDS is informed not to assign time to these selfish nodes. The quantity of dropped packets is less than the unsecured network. Throughput increases, CHs checks their cluster nodes recognize the type and locates the transmission time.

4. Proposed Work

To analyze and prognosticate network data traffic we used AR, ARFIMA and FARIMA [14,15]. Network data traffic predictability analysis provided better predictability then we used multiplexing and low pass filtering. However there is probability of huge error prediction due to large amount of network traffic. Thus, the above mentioned models should be comparatively stable. Sometimes these time series prediction models under the guidance predict trends of network data traffic. Network traffic prediction models are categorized in to existing models and new models. In our designed method we sampled all the network data traffic after gathering network data traffic and flow information.

Let S_n be the state of network traffic, therefore the network traffic sequence will be denoted by:

S_1, S_2, S_3…….. Sx--- S_n

Next we will predict the network data traffic and to achieve a correct and explicit output we must subdue the network data traffic and this can be achieved by preprocessing the data flow by aggregatively averaging sequence S_n with the time session.

$$X_x^-(S_1 + S_2 + S_3 + ... + S_n)/T_x \quad \text{----------I}$$

After calculating the aggregate average, AR model is used to do prediction and is described in the following equation.

$$X_y^\wedge = \sum_{x=1}^{m} axX_{y-x}^- \quad \text{----------II}$$

And after evaluating equation 2, S_x can be predicted and is mentioned below:

$$S_x^\wedge = T_x X_x^\wedge - T_{x-1} X_{y-x}^- \quad \text{----------III}$$

The prediction of S_x is $S^\wedge_x$ and T_x is network traffic's x^{th} sequence. Even from the above formulas we can obtain the prediction error also and can be calculated with the following formula.

$$P.E\square X_x = X_x - S_x^\wedge \quad \text{----------IV}$$

Furthermore, we can use Lyapunav constant to analyze predicted error if we assume that the propagation error is behaving chaotically. Therefore,

$$\lambda_x \approx \{Ln(\square X_x / \square x_0)\}/T_x \quad \text{---------- V}$$

If the result is greater than 0 that is $\lambda_x > 0$ than propagation predicted error is chaotic. This means that the new genuine data traffic is entering the system and this error is not caused by any DDoS attack (4,5). Table 2 describes the results using Lyapunav constant.

Table 2 describes the results using Lyapunav constant.

Result	Status	Reason	Attack status
$\lambda_x > 0$	Chaotic	New data entering the system	No DDoS attack
$\lambda_x = 0$	Result same	No traffic	No attack
$\lambda_x < 0$	Not chaotic	Traffic	Attack

ALGORITHM

Step I	Gather flow information and network data packets
Step II	Using aggregate averaging preprocess the network traffic as in equation 2
Step III	Predict network traffic using AR models
Step IV	Get the prediction error by $\square X_x = X_x - S_x^\wedge$.
Step V	Using chaos theory detect the malicious data by error prediction
Step VI	Using trend artificial neural network detect DDoS

To enhance the detection accuracy neural networks are trained with up-to-date patterns. The basic fact of artificial neural network is that it treats nodes as neurons (Artificial Neurons).

LEARNING CONCEPTS USED IN THE SYSTEM

Supervised Learning is a machine learning technique by which a function is inferred from labeled training data set. This training data set is composed of various training instances. In supervised learning approach, every instance is a combination of an input object (vector usually) and a required value as an output which is also known as supervisory signal [18]. A new set of examples can be produced by the function inferred from the analysis of training data after the application of supervised learning algorithms [19]. The unknown instances class labels are determined correctly by allowing the optimum scenario to algorithms. A reasonable way is needed by learning algorithms to generalize the training data set to unknown circumstances as shown in figure 1 below. Following are the steps to solve the supervised learning problem:

- The training examples must be determined first, by the user before deciding what kind of data should be used as a training set.
- The training data set must represent the real world use of the inferred function. Therefore, the input object sets and the corresponding outputs are gathered, from humans or measurements.
- The learned function input attributes must be determined accurately so as to represent the input objects correctly. Usually, the object is converted into a vector, containing descriptive features about it.
- The structure of the learned algorithm and the learned function must be determined. E.g., to use decision trees or support vector machines.
- After the design completion, execute the algorithm on the collected training data set. Certain control parameters can be adjusted in some supervised learning algorithms.
- The accuracy of the learned function must be evaluated after the learning and adjustment of certain parameters. The performance parameter of a resulting function should be measured on a test set which is separate from the training data set.

A large variety of supervised learning algorithms along with their strengths and weaknesses exists. Nevertheless, no single algorithm is there which suits the most supervised learning problems.

Fig. 1 Supervised learning model

Unsupervised Learning

The vital factor of Neural Networks is their capacity to learn from their environment. The supervisor presents the Neural Networks learner with an input arrangement& a preferred answer. Supervised learning Neural Networks tries to acquire the functional mapping among the input and chosen reply paths[20].

As compared to supervised learning, the goal of unsupervised learning is to find arrangements or matches in the input data without help. Unsupervised learning Neural Network is function which matches inputs to an related goal [21]. Often referred to as an associative memory NN, usually only contains two layers, input and output layers.

fNN : RI ! Rk

On fascinating result of the skinner box experiments (Hebbian Learning Rule), was an explanation of superstitions. Every time a buzzer rang a food pellet was dispensed to the pigeon. The buzzer was rang in random intervals. However by chance in one of the experiments it happened. When bird pecked on a specific pane of glass the buzzer sounded soon after. This happened a few times in a row, by chance. However, the bird kept pecking the pain of glass many hours later in the hope the buzzer would sound..False associations are a common occurrence even in human beings.

Unsupervised learning is the learning assignment of concluding a task to define concealed arrangement from data. Since the samples provided to the learner are not labeled, there is no error or reward signal to assess a possible explanation – this distinguishes unsupervised learning from supervised learning and reinforcement learning. Unsupervised networks are beneficial for examining data without the desired results. They do not have target outputs when neural nets are unsupervised. Unsupervised learning is associated with the problematic estimation of density in statistics. Though, unsupervised learning too includes numerous additional methods that pursue to review and describe main types and features of the data.

The traditional illustration of unsupervised learning is of both natural and artificial neural networks considered by

Donald Hebb's standard, i.e, neurons that fire together wire together.

Self-Organizing neural networks learn by means of unsupervised learning algorithm to find unseen arrangements in uncategorized input data. The unsupervised learning is the way to study and merge information devoid of giving any error signal to assess the possible result. The algorithm is unsupervised learning due to its nonexistence direction. The unsupervised learning could be valuable as it lets the algorithm to search again for those designs matches /patterns which have been ignored in former evaluation.

Implementation and Results

We created two difference scenarios using Opnet 1.5 simulators in the first scenario we created genuine and burst traffic and in the second scenario we created DDoS attack traffic. We executed both the scenarios in simulators and collected the traffic values. Genuine burst traffic is shown in figure 3 and DDoS attack traffic is shown in figure 4. The traffic is increased as the time goes on.

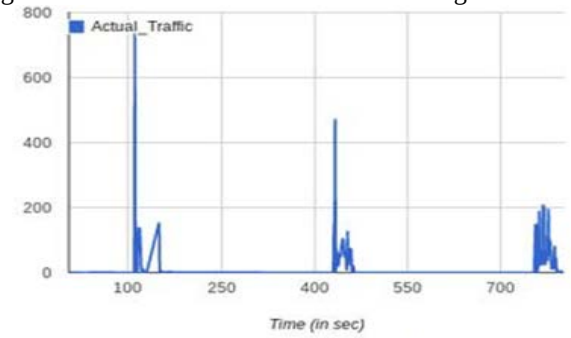

Fig. 3 Legitimate burst traffic

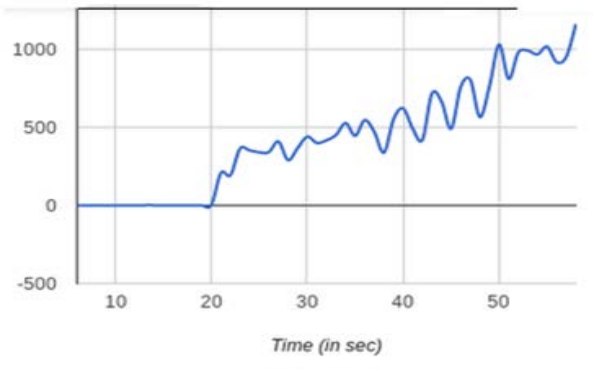

Fig. 4 DDoS attack traffic

We used java SE 1.7 and calculated the Lyapunav coefficient and plotted the graph as shown in figure 5.

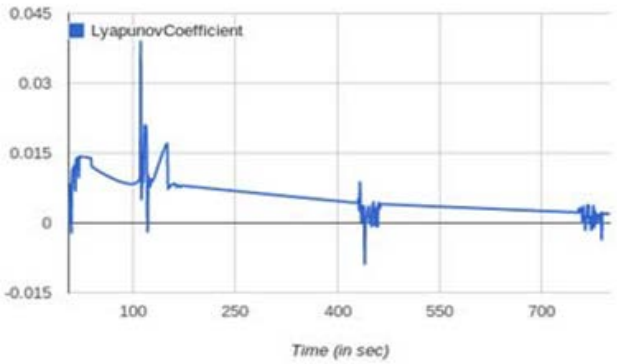

Fig. 5 Traffic chaos pattern- Legitimate burst

In the above figure the values of Lyapunav coefficient are positive at most of the instances with genuine burst traffic patterns.

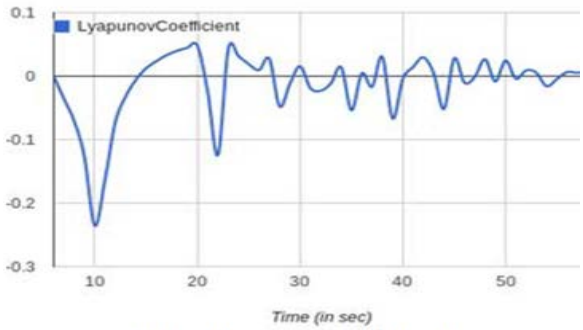

Fig. 6 Traffic chaos pattern- DDoS attack

In the above figure the values of Lyapunav coefficient are negative at most of the instances because of the DDoS attack patterns. Clustering technique is used to do unsupervised learning on traffic data. Different competitive algorithms of network are used to create clusters or similar data groups. Assuming that the three different clusters are DDoS attack, normal data and burst genuine traffic. These clusters (Clustered Data) are used to do supervised learning on traffic data and to reduce the error the famous back propagation algorithm is used. The proposed detection technique using artificial neural network results with greater than 95% accuracy in DDoS attacks detection.

5. Conclusion:

We designed six step algorithm and used chaos theory to detect DDoS attacks effectively. A mirror image of real network environment is used to start the learning process. We launched different DDoS attacks during the flow of the legitimate traffic through the network. We differentiated DDoS attacks and genuine traffic using supervised and unsupervised methods of artificial neural networks. We used Lyapunav coefficient to get the best result in differentiating the legitimate traffic and DDoS attack. We used the up-to-date datasets and trained artificial neural

networks with these two learning method and obtained greater than 95% accuracy in detecting DDoS attacks.

Acknowledgement

This research was funded and conducted at Prince Sattam bin Abdulaziz University, Alkharj, Saudi Arabia during the academic year 2016/2017 under research number 2016/01/6536.

References

[1] Tariq Ahamad, "Detection and Defense Against Packet Drop Attack in MANET" International Journal of Advanced Computer Science and Applications(IJACSA), 7(2), 2016. http://dx.doi.org/10.14569/IJACSA.2016.

[2] Albermany, S.A. &Safdar, G.A. Wireless Personal Communication (2014) 79: 1713. doi:10.1007/s11277-014-1954-1.

[3] Dowd, P.W.; McHenry, J.T., "Network security: it'stime to take it seriously," Computer, vol.31, no.9, pp.24-28, Sep 1998.

[4] Adeyinka, O., "Internet Attack Methods and InternetSecurity Technology," Modeling & Simulation, 2008.AICMS 08. Second Asia International Conference on,vol., no., pp.77-82, 13-15 May 2008.

[5] Marin, G.A., "Network security basics," Security &Privacy, IEEE , vol.3, no.6, pp. 68-72, Nov.-Dec, 2005.

[6] Abdulaziz Aldaej and Tariq Ahamad, "AAODV (Aggrandized Ad Hoc on Demand Vector): A Detection and Prevention Technique for Manets" International Journal of Advanced Computer Science and Applications(IJACSA), 7(10), 2016. http://dx.doi.org/10.14569/IJACSA.2016.071018 -

[7] Agah A, Basu K and K DSajal. Preventing dos attack in sensor networks: a game theoretic approach. In Communications, 2005.ICC 2005. 2005 IEEE International Conference on, volume 5, pages 3218–3222. IEEE, 2005.

[8] Ali, Siti Hajar Aminah, et al. "A neural network model for detecting DDoS attacks using darknet traffic features." Neural Networks (IJCNN), 2016 International Joint Conference on. IEEE, 2016.

[9] B. B. Gupta, Omkar P. Badve, "Taxonomy of DoS and DDoS Attacks and Desirable Defense Mechanism in a Cloud Computing Environment," Neural Computing & Applications, Springer, 2016.

[10] Gupta, B. B., Ramesh Chandra Joshi, and Manoj Misra. "Defending against distributed denial of service attacks: issues and challenges." Information Security Journal: A Global Perspective 18.5 (2009): 224-247.

[11] Saied, Alan, Richard E. Overill, and Tomasz Radzik. "Detection of known and unknown DDoS attacks using Artificial Neural Networks." Neurocomputing 172 (2016): 385-393.

[12] B. B. Gupta, "An Introduction to DDoS Attacks and Defense Mechanisms," Academic Publishing, Germany, ISBN 978-3-8465-9569-5, 2011.

[13] Agrawal, P. K., et. al,. "SVM based scheme for predicting number of zombies in a DDoS attack." Intelligence and Security Informatics Conference (EISIC), 2011 European. IEEE, 2011.

[13] Andrysiak, T., Saganowski, \Lukasz, Choraś, M., & Kozik, R. (2014). Network Traffic Prediction and Anomaly Detection Based on ARFIMA Model. In J. G. de la Puerta, I. G. Ferreira, P. G. Bringas, F. Klett, A. Abraham, A. C. P. L. F. de Carvalho, … E. Corchado (Eds.), International Joint Conference SOCO'14-CISIS'14-ICEUTE'14: Bilbao, Spain, June 25th-27th, 2014, Proceedings (pp. 545–554). Cham: Springer International Publishing. http://doi.org/10.1007/978-3-319-07995-0_54

[14] Gerhard Munz, Georg Carle "Real-time analysis of flow data for network attack detection," IEEE international symposium, 2007.

[15] Chonka, J. Singh, and W. Zhou, "Chaos theory based detection against network mimicking DDoS attacks," IEEE Communication Letters., vol. 13, no. 9, pp. 717–719, 2009.

[16] Yonghong Chen, Xinlei Ma, Xinya Wu, "DDoS detection algorithm based on pre-processing network traffic predicted method and Chaos theory," IEEE Communications Letters, vol. 17, no. 5, May 2013.

[17] Polikar R, Udpa L, Udpa S, Honavar V,"Learn++: An Incremental Learning Algorithm for Supervised Neural Networks",IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS—PART C: APPLICATIONS AND REVIEWS, VOL. 31, NO. 4, NOVEMBER 2001

[18] A. P. Engelbrecht and R. Brits, "A clustering approach to incremental learning for feedforward neural networks," in Proc. Int. Joint Conf. Neural Netw., vol. 3, 2001, pp. 2019–2024.

[19] LukošEvičIus, Mantas, and Herbert Jaeger. "Reservoir computing approaches to recurrent neural network training." Computer Science Review 3.3 (2009): 127-149.

[20] Deng, Li, Geoffrey Hinton, and Brian Kingsbury. "New types of deep neural network learning for speech recognition and related applications: An overview." 2013 IEEE International Conference on Acoustics, Speech and Signal Processing. IEEE, 2013.